

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-247086

(43)Date of publication of application : 19.09.1997

(51)Int.Cl.

H04B 10/00
G01J 9/00
G02F 1/39
G09C 1/00
H04L 9/08
H04L 9/38

(21)Application number : 08-052102

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 08.03.1996

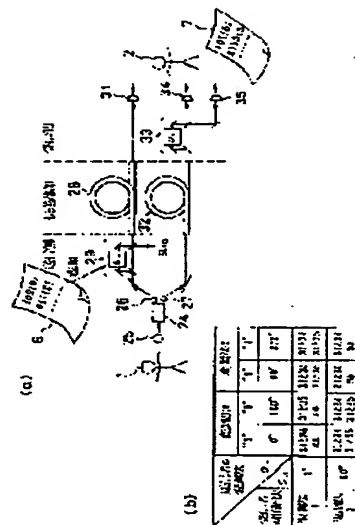
(72)Inventor : IMOTO NOBUYUKI
KOASHI MASATO
MAIKERU UERUNAA

(54) CONSTITUTION METHOD FOR QUANTUM PASSWORD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the constitution method of a quantum password, which does not require a highly precise synchronous clock, by using a remote quantum correlation without using polarization and executing simultaneous measurement only on a receiver-side.

SOLUTION: A transmitter 1 generates photons 26 and 27 from a pump photon 25 by using an optical parametric amplifier 24. The photon 26 is transmitted to an optical fiber 28 after it passes through a delay 29 and the photon 27 is transmitted to an optical fiber 32. On a reception-side, the photon 26 is counted in a light receiver 31 and the photon 27 is counted in a light receiver 34 or 35 after it passes through a delay 33. The signals are simultaneously counted in the light receiver 31 and the light receiver 34 or 35. Whether a phase difference which the delay 29 gives and that which the delay 33 gives are a specified combination or not is recognized by a classic channel. Only when it is the specified combination, the signal of one bit is registered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平 9 - 2 4 7 0 8 6

(43)公開日 平成9年(1997)9月19日

(51)Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 B	10/00		H 0 4 B	9/00 Z
G 0 1 J	9/00		G 0 1 J	9/00
G 0 2 F	1/39		G 0 2 F	1/39
G 0 9 C	1/00	6 3 0	G 0 9 C	1/00 6 3 0 C
		7259- 5 J		6 3 0 Z
		7259- 5 J		
審査請求 未請求 請求項の数 3			O L	(全 1 1 頁) 最終頁に続く

(21)出願番号 特願平8-52102

(22)出願日 平成8年(1996)3月8日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 井元 信之

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 小芦 雅斗

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 マイケル・ウェルナー

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

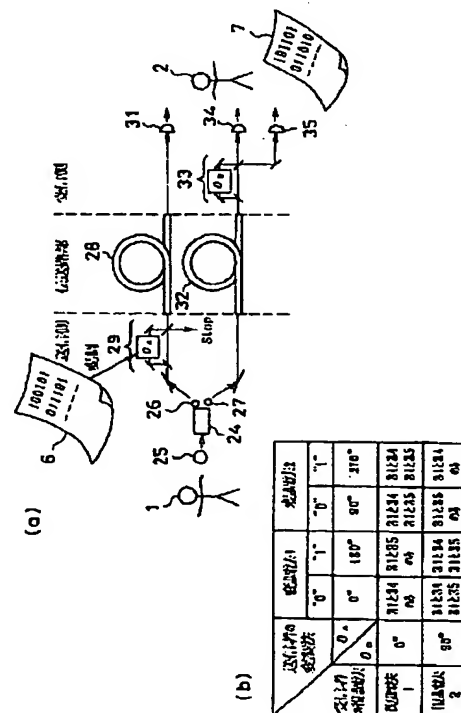
(74)代理人 弁理士 三好 秀和 (外1名)

(54)【発明の名称】量子暗号の構成方法

(57)【要約】

【課題】 偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを必要としない量子暗号の構成方法を提供する。

【解決手段】 送信者1は光パラメトリック増幅器24を用いてポンプ光子25から光子26、27を発生し、光子26は遅延29を通過後光ファイバ28に送り、光子27は光ファイバ32に送る。受信側で光子26を受光器31でカウントし、光子27は遅延33を通過後受光器34または35でカウントする。受光器31と受光器34または35で信号が同時にカウントされ、しかも遅延29が与える位相差と遅延33が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録する。



【特許請求の範囲】

【請求項1】 量子力学状態を変調した第1の信号を伝える量子チャンネルと、古典状態を変調した第2の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第1の信号に発生する攪乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、

送信側において、同一の時間幅を有し、前記時間幅より長いコヒーレント時間を有し、それぞれが1つの光子からなる第1および第2の光パルスを発生し、

前記第1の光パルスを2つの光路に分岐し、分岐後の光パルスの一方に前記時間幅より長く前記コヒーレント時間より短い第1の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を第1の量子チャンネルに光学的に接続し、

前記第2の光パルスを第2の量子チャンネルに入力し、受信側においては、前記第1の量子チャンネルの出力を第1の光検出手段に入力し、

前記第2の量子チャンネルの出力を2つの光路に分岐し、分岐後の光パルスの一方に、前記第1の時間遅延との差が前記時間幅より小さい第2の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の光検出手段に入力し、他方の光路を第3の光検出手段に入力し、前記第1の光検出手段と第2または第3の光検出手段で信号が同時に検出され、しかも前記第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録することを特徴とする量子暗号の構成方法。

【請求項2】 前記第1および第2の光パルスを光パラメトリック増幅または原子のカスケード遷移によって発生することを特徴とする請求項1記載の量子暗号の構成方法。

【請求項3】 量子力学状態を変調した第1の信号を伝える量子チャンネルと、古典状態を変調した第2の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第1の信号に発生する攪乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、

送信側において、ポンプ光子を光パラメトリック増幅器に供給して、第1の光パルスおよび第2の光パルスを発生し、

第1の光子パルスを2つの光路に分岐し、分岐された一方の光パルスに遅延手段で第1の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を光ファイバか

らなる第1の量子チャンネルに光学的に接続し、

前記第2の光パルスを光ファイバからなる第2の量子チャンネルに入力し、

受信側においては、前記第1の量子チャンネルの出力を第1の受光器に入力し、

前記第2の量子チャンネルの出力を2つの光路に分岐し、分岐された一方の光パルスに遅延手段により第2の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の受光器に入力し、他方の光路を第3の受光器に入力し、

前記第1の受光器と第2または第3の受光器で信号が同時に検出され、しかも前記第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録することを特徴とする量子暗号の構成方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、量子力学の不確定性原理を利用し、盗聴者に有無をモニタしながら鍵である乱数列を交換する量子暗号の構成方法に関する。

【0002】

【従来の技術】暗号には、盗聴されていることを前提にその解読が計算量論的に困難であることに安全性の根拠を置く現代暗号と、量子力学の不確定性原理を利用し、盗聴者の有無をモニタしながら鍵である乱数列を交換することを特徴とする量子暗号とがある。まず、現代暗号について説明する。

【0003】現代暗号は、送信するメッセージをデジタル化し（これを平叙文と呼ぶ）、それに乱数を演算して第三者にはランダムに見える暗号文にし、第三者の知らない復号法で受信者が復号するもので、大きく分けて秘密鍵暗号法と公開鍵暗号法がある。送信者が暗号化に使う乱数表を暗号鍵、受信者が復号に使う乱数表を復号鍵と呼ぶが、秘密鍵暗号法では暗号鍵と復号鍵は同一（秘密鍵と呼ばれる）であり、送信者と受信者は何らかの安全な方法、例えば直接会うなどで事前に秘密鍵を決定している。

【0004】平叙文と秘密鍵の長さが等しいとき、すなわち一度使った秘密鍵は必ず捨てるとき（これをone time pad法と呼ぶが）、この方法は絶対的安全性を有していることがShannonにより証明されている。しかし、メッセージに匹敵する長さの秘密鍵をその都度事前に交換することの非現実性（それができればメッセージそのものを交換すればよい）の故、one time pad法は実際には使われていない。実用的な秘密鍵暗号法では同じ秘密鍵を繰り返し使用する。

【0005】公開鍵暗号法では受信者が公開鍵と秘密鍵の2つを所有しており、公開鍵を一般に公開する。送信

者は受信者の公開鍵を使って暗号化し送信し、受信者は秘密鍵を使って復号化する。いうまでもなく、ここでも公開鍵と秘密鍵を繰り返し使用する。これらの現代暗号については文献：[1] 太田和夫・黒澤馨・渡辺治著「情報セキュリティの科学」（講談社ブルーバックス）、[2] 今井秀樹著「暗号のおはなし」（日本規格協会）、[3] 岡本英司著「暗号理論入門」（共立出版）、[4] 池野信一、小山謙二著「現代暗号理論」（電通通信学会）に詳しく説明されている。

【0006】現代暗号では暗号文が盗聴されることを前提としており、盗聴されても解読に天文学的時間がかかることに安全性の根拠を置いている。計算量論的表現を用いれば、整数の素因数分解がP型問題に属していないという仮説に根拠を置いている。

【0007】しかし、この仮説は未だ証明されていない予想に過ぎない。それどころか1994年には量子コンピューティング法まで計算法を拡張すれば、素因数分解がP型問題に転化されることが数学的に証明された。これについては文献：[5] Peter W. Shor: "Algorithms for quantum computation: Discrete logarithms and factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, CA, 1994) p.124、[6] 西野哲朗「量子コンピュータ」情報処理学会誌第36巻4号(1995年4月)p.337に詳しく説明されている。

【0008】この量子コンピュータは未だ実用化されていないが、現代暗号の究極の拠り所が理論上とはいえ崩れ去ったため、その安全性が将来保証されなくなることが避けられないと考えられている。

【0009】次に、従来の量子暗号について説明する。

【0010】量子コンピューティング法を用いても、なお破ることができない暗号として量子暗号がある。これは量子力学の不確定性原理に基づき盗聴者のどんな盗聴行為も必ず何らかの痕跡を量子レベルの信号に残すことを利用し、盗聴されていないことを確認しながら秘密鍵を決定する手続きである。すなわち、上述した秘密鍵暗号方式において送信者と受信者が何らかの安全方法で事前に秘密鍵を決定しておく必要があるが、その安全な方法としては、直接会見を除けば現在のところ量子暗号以外はない。量子暗号を用いれば恒常的に秘密鍵の交換を行うことが可能であり、絶対安全が保証されているone time pad法の使用が可能となる。

【0011】量子暗号の具体的方法として4偏光状態暗号、2コヒーレント状態暗号、4コヒーレント状態暗号、時間差干渉暗号、二光子干渉暗号が提案されている。次に、これらの各量子暗号について説明する。

【0012】まず、4偏光状態暗号について説明する。4偏光状態暗号は最初に考案された量子暗号であり、詳細は文献：[7] C.H. Bennett and G. Brassard, in Proce

edings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.175、[8] A. エカート／井元信之訳「量子暗号への招待」バリティ、vol.7, No. 2, p.26 (1992)、[9] G. コリンズ／井元信之訳「量子暗号は史上最強の暗号」バリティ、vol.8, No.5, p.31 (1993)に述べられているが、以下簡単に説明する。

【0013】4偏光状態暗号においては、図2に示すように、送信者1と受信者2は1ビットにつき光子を1つだけ含む光パルス3を送る量子チャンネル4と送信および受信状況を確認し合う古典的チャンネル5を使う。量子チャンネル4は通常光ファイバであり、古典的チャンネル5は無線や電話等である。古典的チャンネル5は盗聴されていることを前提とするが、改竄はされないと仮定する。このことを明確にするため、以下本明細書では古典的チャンネルを公開チャンネルと呼ぶ。また、量子暗号に限らず暗号理論の前提として、盗聴者は図の伝送路部にアクセスすることはできるが、送信側および受信側にはアクセスできない。送信側ビット“0”および“1”を光パルス3にコーディングするにあたり、直線偏光と円偏光の2種類の変数、すなわち2種類のコーディング法を用いる。例えば、図3に示すように、直線偏光コーディングの場合は「水平」を“0”に、「垂直」を“1”に、円偏光コーディングの場合は「右回り」を“0”に、「左回り」を“1”に対応させる。このような取り決めを送信者1と受信者2は予め（公開チャンネル5で）行っておく。送信者1は二進法で書かれた乱数表6を用意する。これは受信者2と共有する秘密鍵7を生成するための元になる乱数表である。秘密鍵7は次に説明するように乱数表6から半分弱のビットを抽出した部分乱数表となっている。4偏光状態暗号における送信者1と受信者2のプロトコルは次のようになる。

【0014】ステップ1：送信者1はランダムにコーディング法を選択し、乱数表6に従って光パルス3の偏光を変調器8を用いて変調する。例えば円偏光でコーディングすることとし、乱数表6の最初の値が“1”ならば「左回り」偏光となるように光パルス3の偏光状態を変える。送信者1には選択したコーディング法は知らせず、光パルス3だけを送る。同様にして引き続くビットに対して次々と光子を送る。

【0015】ステップ2：受信者2は受けた光パルス3が光子を1つしか含まないので、直線偏光と円偏光の両方を測ることはできない（不確定性原理）。従って、どちらを測るかを決し、偏光測定器を含む受光器9を用いて測定する。送信者1が選択したコーディング法と同じコーディング法と間違ったコーディング法を選ぶ確率はそれぞれ50%である。同じだった場合、乱数表6の値が正しく受信者2に再現されるが、間違った場合はそのビットに関する送信者1と受信者2の間の相互情報量

10

20

30

40

50

はゼロとなる。

【0016】ステップ3：光パルスを1つ測定する毎に（あるいは後でまとめて交信してもよいが）受信者2はどちらのコーディング法を選択したか、公開チャンネル5で明らかにする。送信者1はそれを聞き、受信者2のコーディング選択が正しかったか否かを公開チャンネル5で伝える。

【0017】ステップ4：送信者1と受信者2は双方が同じコーディング法を選択した約半分のビットだけを採用し、後の半分は捨てる。盗聴がなければ双方に同じ乱数表が形成されているはずである。

【0018】ステップ5：送信者1と受信者2は残ったビットのうち適当な割合で照合ビットを抽出し、それぞれの答合わせを（公開チャンネル5で）行う。十分な数の照合ビットが一致すれば、上記文献に説明されているような理由により、1に近い確率で盗聴されていないと結論づけられる。

【0019】ステップ6：照合ビットも除いたビットは送信者1と受信者2しか知らない同一の値を有することが保証されているので、それを秘密鍵7と決定する。

【0020】以上の手順により、盗聴されていないことをリアルタイムでモニタしながら秘密鍵を生成して行くことができる。万一照合ビットから盗聴を発見した場合は、盗聴発見期間の交信をすべて無効とし、量子チャンネルをチェックするか、あらためて構築する。実際は盗聴者が最も恐れるのは盗聴の発覚であり、しかも発覚の危険を侵しても盗聴遂行できない（盗聴した秘密鍵は破棄されてしまう）ので、量子暗号に対して盗聴者のなすべき手段は事実上ない。

【0021】なお、量子暗号の実用性を示す特徴の1つとして、伝送路損失の存在が致命的でないという事情についてここで触れておきたい。光の量子状態を制御する通信や情報処理においては伝送路の損失あるいは光検波器の不完全な量子効率により量子状態が大きく破壊されてしまうことが致命的欠陥であることが知られている。意味を持つメッセージを送信したり処理したりする場合は、量子状態の破壊は情報そのものの破壊を意味する。しかし、量子暗号はまず乱数表の交換が目的であるので、伝送損失等により光子が欠落しても乱数表が間引きされるに過ぎない。損失の影響は主に伝送レートが下がることに現れるだけであり、上記プロトコルの有効性には影響しない。このような特徴は4偏光状態暗号に限らず、量子暗号すべてに共通する特徴である。

【0022】4偏光状態量子暗号を実用化する際に最も重要となるのは、光子が伝送路を通過する間に予測不能な偏光の攪乱があつてはならないことである。この攪乱を避けるためにいわゆる偏光保存ファイバを用いることはできない。偏光保存ファイバは直交する特定の2つの偏光を保存するだけであり、4偏光状態暗号で用いられるような直交しない組合せも含む4つの偏光をすべて保

存することはできない。一方偏光を保持しないファイバは偏光の時間的揺らぎが避けられない。揺らぎを時間追跡して偏光補償する技術はあるが、ただ1つの光子を送受信する場合には適用できない。送信偏光が受信偏光に誤って伝えられた場合、照合ビットの矛盾と秘密鍵生成エラーの原因となる。すなわち、照合ビットの矛盾が発見された場合、測定誤りと盗聴による2つの原因を峻別しなければならないが、それは一般に困難であり、複雑な誤り訂正手続きの導入が避けられない。更に盗聴でなく測定誤りと判定され秘密鍵を破棄しない場合も、測定誤りによる秘密鍵の生成エラーを起こしている可能性がある。

【0023】次に、2コヒーレント状態暗号について説明する。2コヒーレント状態暗号は2状態量子暗号の一例である。詳細は文献：[10] C.H.Bennett, Phys. Rev. Lett. 68, 3121 (1992)、[11] B.Huttner, N.Imoto, N.Gisin, and T.Mro, Phys. Rev. A 51, 1863 (1995) に述べられており、文献[10]で提案された構成は図5に示すものであるが、説明のためにより簡略化した図4でまず説明する。

【0024】図4において、送信者1は光パルス3を50%のビームスプリッタ10で光パルス11と12に分け、位相変調器13を用いて光パルス11の光位相を乱数表6に従ってビット値が“0”ならば0、ビット値が“1”ならば180度と変調し、光ファイバ14と15からなる量子チャンネル4に送る。以下すべての量子暗号において公開チャンネル5は共通であるので、以降本明細書では省略する。

【0025】受信者2は、50%のビームスプリッタ16で光パルス11および12を干渉させる（実際は文献[10]にも述べられているようにビームスプリッタ10および16の反射率は50%である必要はない）。ビームスプリッタ10からビームスプリッタ16までは1つのマッハツェンダー干渉計を構成する。受信者2は光ファイバ14と15の間の位相差 θ を適当に調節し、ビームスプリッタ16においてビット値“0”のパルスは受光器17側がダークフリンジに、ビット値“1”のパルスは受光器18側がダークフリンジになるようにする。

【0026】2コヒーレント状態暗号では、光パルス3に含まれる平均光子数が1よりずっと小さい（例えば0.1の）コヒーレント状態の光を用いる。これは光パルス3に含まれる光子の数が2以上になる確率をできる限り0に近づけるためである。平均光子数が1よりずっと小さいので、パルス到着時に受光器17と18の何れにも光子がカウントされないケースがほとんどとなるので、ほとんどの場合受信者2にとってビット値判定不能となる。しかし、受光器17でカウントされた場合はビット値は“1”、受光器18でカウントされた場合は“0”であると確定的に結論することができる。以上のことから次のようなプロトコルで秘密鍵交換が可能であ

10

20

30

40

50

る。

【0027】ステップ1：送信者1は乱数表6に従って光パルス11の位相を位相変調器13を用いて変調し、送る。

【0028】ステップ2：受信者2は受光器17と18で光子のカウンティングを行う。カウントした場合、受光器17と18のどちらでカウントしたかは言わず、カウントした事実だけを公開チャンネルで送信者1に告げる。

【0029】ステップ3：盗聴がないと仮定すれば、送信者は受信者が受光器17と18のどちらでカウントしたか知っているので、そのようなビット列から適当な割合で照合ビットを抽出し、それぞれの答合わせを（公開チャンネル5で）行う。十分な数の照合ビットが一致すれば、後で述べる理由により1に近い確率で盗聴されていないと結論づけられる。

【0030】ステップ4：照合ビットを除いたビットは送信者1と受信者2しか知らない同一の値を有することが保証されているので、それを秘密鍵7と決定する。

【0031】このスキームに対し盗聴者が何ができるかを考える。量子チャンネル4にアクセスして二手に分かれた光パルスの位相差を測定するためには、受信者と同様干渉させて光子のカウンティングを行う必要がある。たまたまカウンティングに成功すれば、送信者と同じ装置を用いて送信者が送ったのと同じ並列2パルスを送ることができる。しかし、ほとんどのパルスで光子がカウントされないので、その場合は偽のパルスを何も送らないか、ランダムな位相差を持った偽のパルスを送るかしかない。前者の場合、伝送レートが本来値から下がり、後者の場合照合ビットの矛盾を引き起こし、いずれにせよ送信者と受信者から検知される。

【0032】2コヒーレント状態量子暗号を実用化するには、長い伝送路を含むマッハツェンダー干渉計において、伝送路の揺らぎによる位相差揺らぎをいかに安定化させるかが重要となる。図4のように2本の光ファイバを用いたのでは500mを越すあたりから干渉計の安定化は不可能となる【文献12：井元信之「光子数の量子非破壊測定の研究」博士論文（東京大学）】。そこで光パルス11と12に時間差をつけて1本の光ファイバに通すことが考えられる【文献10】。

【0033】図5にその場合の構成を示す。図5において、送信者1は光パルス3を偏光ビームスプリッタ19により直交する偏光関係にある等強度のパルス11と12に分ける。パルス11を位相変調器13で変調し、パルス12はそのまま偏光ビームスプリッタ20を介して偏光保存ファイバ4に入射する。このようにしてパルス11と12は遅延を持った二連パルスとして光ファイバ4の中を伝わり、受信者側では偏光ビームスプリッタ21で二連パルスを分離し、逆遅延をかけた後、偏光ビームスプリッタ22でパルス11と12を干渉させる。光

パルス11と12は光ファイバ4の中を伝搬する間に同じ位相揺らぎを受けるので、干渉させるときには揺らぎが打ち消し合う。光ファイバの位相揺らぎの周波数特性は約1GHzまでと考えられるので、その揺らぎの影響を受けないためには、パルス11と12の間隔は1ns以下でなければならない。この場合の困難は、そのような極短二連パルスを可干渉性を失わないように発生することにある。

【0034】次に、4コヒーレント状態暗号について説明する。4コヒーレント状態暗号は、上述した4偏光状態暗号と2コヒーレント状態暗号の特長を組合せ、いずれよりも大幅な性能改善を図ったものであり、詳細は文献11に述べられている。構成的には図4の2コヒーレント状態暗号において位相変調を0度、90度、180度、270度の4種類を用い、プロトコルとしては受信者が光子をカウントしたか否かの事実に加えて（0度、180度）のペアと（90度、270度）のペアのいずれを選択したかを送信者と受信者が突き合わせるというプロトコルを付加した暗号である。詳しい動作および性能の比較は文献11に詳しく解析されている。容易に推測されるように、この量子暗号法の欠点は上述した2コヒーレント状態暗号と同じ欠点を有している。

【0035】次に、時間差干渉暗号について説明する。時間差干渉暗号は図4に示すようにマッハツェンダー干渉計を用いる点で図4の2コヒーレント状態暗号に類似しているが、他の量子暗号が非直交状態を用いるのに対し、直交する状態のみを用いる点が特徴的である。詳細は文献：[13] Goldenberg and Vaidmann: Phys. Rev. Lett. 75, 1239 (1995) に述べられているが、以下簡単に説明する。図6に示すように、送信者1はビット“0”の場合はポートA側から、ビット“1”の場合はポートB側から光パルス3を入れ、乱数表6を送る。光パルス3は光子をただ1つ含むとする。光パルス3は50%ビームスプリッタ10で二手に分かれ、光パルス11はそのまま光ファイバ14に、光パルス12は長い遅延23を経て光ファイバ15に入る。遅延を伝送距離より長くしておくことにより光パルス11が受信者側に到着した後光パルス12が伝送路部に入る。

【0036】受信者側では光パルス11に遅延23と同じ長さの遅延24を設ける。これにより50%ビームスプリッタ16において光パルス11と12は干渉し、ポートA側から入射した光パルス3はポートA'に、ポートB側から入射した光パルス3はポートB'に出射する。受信者2は単にポートA'かB'かを見ているだけで送信者1の乱数表6を再生できる。照合ビットの棄却や伝送損失による光子の欠落を除き、送信者と受信者は秘密鍵7を構築できる。盗聴者は伝送路部で光パルス11と12に同時にアクセスすることはできず、光パルス11を測定・加工した後、光パルス12を測定・加工することしかできない。文献13に詳しく述べられている

通り、この制約の下ではビット“0”と“1”を破壊せずに読み取る手段がない。

【0037】文献13にも述べられている通り、この量子暗号は直交する状態のみを用いるという原理的興味で提案されたもので、実用性には乏しい。時間差を設けることが本質的であるので図5のような二連パルスを使うことができず、二本の伝送路を用いる以外にない。そのようなマッハツェンダー干渉計を安定化するためには伝送距離を数百m以下とせざるを得ない。

【0038】次に、二光子干渉暗号について説明する。二光子干渉暗号はフランソン干渉計と呼ばれる二光子干渉計を利用する量子暗号で、文献：14 [A.E.Ekert et al., Phys. Rev. Lett. 69, 1293 (1992)] で提案された。図7はその動作を説明する図である。24は光パラメトリック増幅器であり、角振動数 ω_p のポンプ光と呼ばれる光子25を吸収し、角振動数 ω_a と ω_b の光子を1つずつ発生する。それぞれの光子パルスを26および27とする。光子パルス26は光ファイバ28に送られ、遅延29を通過後受光器30または31でカウントされる。光子パルス27は光ファイバ32に送られ、遅延33を通過後受光器34または35でカウントされる。遅延29から先は送信者側、遅延33から先は受信者側である。図のように送信者1と受信者2について対称な構成であるので、送信者あるいは受信者という名称は最良ではないが、他の量子暗号と用語を統一するためこれらの名称を用いる。位相差 θ_a は送信者側で調節し、位相差 θ_b は受信者側で調節する。光パラメトリック増幅器24は送信者側と受信者側のいずれに回してもよいが、盗聴者はアクセスできないようにしておく。今、送信者と受信者が($\theta_a + \theta_b = 0$)となるように位相調整することを取り決めれば、フランソン干渉計の原理すなわち遠隔量子相関により、受光器30と35で光子が同時カウントされる確率や受光器31と34で同時カウントされる確率は0となる。従って受光器30と34で同時カウントがあるか、受光器31と35で同時カウントがあるか、あるいは同時カウントがないかのいずれかしか起きない。そこで、送信者と受信者が同時にカウントしたか否かのみを公開チャンネルで確認し合うだけで、送信者と受信者はそれぞれどの受光器でカウントしたかを互いに知る。このようにして共通の乱数表を構築できるので、ときどきビット照合して盗聴のないことを確認した残りのビットを秘密鍵として採用することができる。この方式では乱数表を用いて送信者が何らかの物理量を意図的に変調するプロセスはない。なぜならば、受光器31と受光器34で光子の同時カウントがあるか受光器31と受光器35で光子の同時カウントがあるかは、量子力学的確率過程として決まるからである。

【0039】この量子暗号は実用的見地から優れた特徴をいくつか有している。まず、 θ_a と θ_b が空間的にまったく独立であり、大きなマッハツェンダー干渉計の内

部にあるわけではないので、伝送路の揺らぎと無関係に送信者と受信者が独立に調整できることである。また、偏光を使っていないので、任意偏光を保存する必要はなく、特定の偏光を保存する偏光保存ファイバを使うことができる。このためフランソン干渉計の安定化は極めて容易であり、しかも送信者と受信者が別個に安定化すればよい。

【0040】この量子暗号の実用上の問題点は、遠く離れた送信者と受信者がカウントした光子が同時刻にカウントされたか遅延があったかを区別しなければならないことにある。遅延28および32はナノ秒のオーダーであるから(それ以上長くすると θ_a や θ_b の揺らぎを生ずる)、その程度の時間分解能で送信者と受信者のクロックを同期させる必要がある。これは一般に高価な設備を必要とする。

【0041】

【発明が解決しようとする課題】上述したように、従来の量子暗号法のうち、4偏光状態暗号は、任意の偏光を保存するファイバを必要とするという問題がある。また、2コヒーレント状態暗号、4コヒーレント状態暗号、および時間差干渉暗号は、長距離マッハツェンダー干渉計の安定化を必要とし、更に二光子干渉暗号は、送信者と受信者間で高精度の同期クロックを必要とするという問題がある。

【0042】本発明は、上記に鑑みてなされたもので、その目的とするところは、偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを必要としない量子暗号の構成方法を提供することにある。

【0043】

【課題を解決するための手段】上記目的を達成するため、請求項1記載の本発明は、量子力学状態を変調した第1の信号を伝える量子チャンネルと、古典状態を変調した第2の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第1の信号に発生する攪乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、送信側において、同一の時間幅を有し、前記時間幅より長いコヒーレント時間を有し、それぞれが1つの光子からなる第1および第2の光パルスを発生し、前記第1の光パルスを2つの光路に分岐し、分岐後の光パルス的一方に前記時間幅より長く前記コヒーレント時間より短い第1の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を第1の量子チャンネルに光学的に接続し、前記第2の光パルスを第2の量子チャンネルに入力し、受信側においては、前記第1の量子チャンネルの出力を第1の光検出手段に入力し、前記第2の量子チャンネルの出力を2つの光路に分岐し、分岐後の光パルス的一方に、

前記第1の時間遅延との差が前記時間幅より小さい第2の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の光検出手段に入力し、他方の光路を第3の光検出手段に入力し、前記第1の光検出手段と第2または第3の光検出手段で信号が同時に検出され、しかも前記第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録することを要旨とする。

【0044】請求項1記載の本発明にあつては、送信側において、第1および第2の光パルスを発生し、第1の光パルスを2つの光路に分岐し、分岐後の光パルスの一方に第1の時間遅延を施して、他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を第1の量子チャンネルに光学的に接続し、第2の光パルスを第2の量子チャンネルに入力し、受信側においては、第1の量子チャンネルの出力を第1の光検出手段に入力し、第2の量子チャンネルの出力を2つの光路に分岐し、分岐後の光パルスの一方に第2の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の光検出手段に入力し、他方の光路を第3の光検出手段に入力し、第1の光検出手段と第2または第3の光検出手段で信号が同時に検出され、しかも第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録する。

【0045】また、請求項2記載の本発明は、請求項1記載の発明において、前記第1および第2の光パルスを光パラメトリック増幅または原子のカスケード遷移によって発生することを要旨とする。

【0046】更に、請求項3記載の本発明は、量子力学状態を変調した第1の信号を伝える量子チャンネルと、古典状態を変調した第2の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第1の信号に発生する攪乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、送信側において、ポンプ光子を光パラメトリック増幅器に供給して、第1の光パルスおよび第2の光パルスを発生し、第1の光子パルスを2つの光路に分岐し、分岐された一方の光パルスに遅延手段で第1の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を光ファイバからなる第1の量子チャンネルに光学的に接続し、前記第2の光パルスを光ファイバからなる第2の量子チャンネルに入力し、受信側においては、前記第1の量子チャンネルの出力を第1の受光器に入力し、前記第2の量子チャンネルの出力を2つの光路に分岐し、分岐

された一方の光パルスに遅延手段により第2の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の受光器に入力し、他方の光路を第3の受光器に入力し、前記第1の受光器と第2または第3の受光器で信号が同時に検出され、しかも前記第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録することを要旨とする。

【0047】請求項3記載の本発明にあつては、送信側において、ポンプ光子を光パラメトリック増幅器に供給して第1の光パルスおよび第2の光パルスを発生し、第1の光子パルスを2つの光路に分岐し、一方の光パルスに第1の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路のうちの1つの光路を光ファイバからなる第1の量子チャンネルに光学的に接続し、第2の光パルスを光ファイバからなる第2の量子チャンネルに入力し、受信側においては、第1の量子チャンネルの出力を第1の受光器に入力し、第2の量子チャンネルの出力を2つの光路に分岐し、一方の光パルスに第2の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る2つの光路の一方を第2の受光器に入力し、他方の光路を第3の受光器に入力し、第1の受光器と第2または第3の受光器で信号が同時に検出され、しかも第1の時間遅延が与える位相差と第2の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、1ビットの信号を登録する。

【0048】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0049】図1(a)は、本発明の一実施形態に係る量子暗号の構成方法を説明する図である。同図に示す本実施形態の量子暗号の構成方法は、フランソン干渉計の原理をベースに新しい量子暗号の構成およびプロトコルを考案したものであり、偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを不要にしたものであり、従来の二光子干渉量子暗号の優れた特徴をそのまま保有しているものである。

【0050】図1(a)において、送信者1は光パラメトリック増幅器24を用い、角振動数 ω_p のポンプ光子25を角振動数 ω_a の光子26と角振動数 ω_s の光子27を発生する。光子26は遅延29を通過後光ファイバ28に送り、光子27はそのまま光ファイバ32に送る。受信側では光子26をそのまま受光器31でカウントし、光子27は遅延33を通過後受光器34または35でカウントする。位相差 θ_a は送信者側で変調(固定調節でなくビット毎に)し、位相差 θ_s は受信者側で変

調する。その取り決めについては後述する。

【0051】フランソソ干渉計の原理、すなわち遠隔量子相関によれば、 $\theta_A + \theta_B$ が0または180度の場合は、同時カウントがあるとすれば受光器31と34に限られ、 $\theta_A + \theta_B$ が90度または270度の場合は、同時カウントがあるとすれば受光器31と35に限られる。この事実を用いることにより、4偏光状態暗号プロトコルと類似のプロトコルを用いて量子暗号を実現することができる。

【0052】まず、送信者1は二種類の変調法から1つを選択する。変調法1ではビット“0”のとき $\theta_A = 0$ 、“1”のとき $\theta_A = 180$ 度とし、変調法2ではビット“0”のとき $\theta_A = 90$ 度、“1”のとき $\theta_A = 270$ 度とする。変調法1と2に対応し、受信者側では復調法1として $\theta_B = 0$ 、復調法2として $\theta_B = 90$ 度のうちから選択する。送信者と受信者の選択の可能な組合せに対し同時カウントが起り得る受光器のペアを図1(a)に示した。この図から、送信者の変調法と受信者の復調法が一致した場合にのみ、同時カウントのある受光器ペアが一意に定まることが分かる。変調法と復調法が一致しない場合は情報の伝達が行われない。具体的プロトコルは次の通りである。

【0053】ステップ1：送信者1はランダムに変調法を選択し、乱数表6に従って θ_A を変調する。

【0054】ステップ2：受信者2は送信者1と独立にランダムに復調法を選択し、 θ_B を設定する。受光器31と34または31と35のいずれかのペアで光子の同時カウントが起り得る。

【0055】ステップ3：同時カウントを観測する毎に（あるいは後でまとめて通信してもよいが）受信者2はどちらの復調法を選択したか、公開チャンネルで明らかにする。送信者1はそれを聞き、受信者2の復調法選択が正しかったか否かを受信者2に明らかにする。

【0056】ステップ4：送信者1と受信者2は双方が対応する変復調法を選択した約半分のビットだけを採用し、後の半分は捨てる。盗聴がなければ双方に同じ乱数表が形成されているはずである。

【0057】ステップ5：送信者1と受信者2は残ったビットのうち適当な割合で照合ビットを抽出し、それぞれの答合わせを行う。十分な数の照合ビットが一致すれば1に近い確率で盗聴されていないと結論づけられる。

【0058】ステップ6：照合ビットも除いたビットは送信者1と受信者2しか知らない同一の値を有することが保証されているので、それを秘密鍵7と決定する。

【0059】

【発明の効果】以上説明したように、本発明によれば、位相差 θ_A と θ_B が空間的にまったく独立で伝送路の揺らぎと無関係に送信者と受信者が独立に調整できるので、長距離マッハツェンダー干渉計の安定化のような送信者と受信者を包括して調整を行う必要がない。また、偏光を使っていないので、任意の偏光を保存する光ファイバを要求しない。更に、本発明では光子の同時カウントを受信者側のみで行うため、受信者がローカルなクロックを持っていればよい。これは送信者と受信者の間で高精度の同期クロックが必要であった従来の二光子干渉量子暗号と大きく異なる点である。このように、本発明は上述した従来の量子暗号の欠点をすべてクリアする新しい量子暗号の構成方法を実現することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る量子暗号の構成方法を説明するための図および本実施形態における光子の同時カウンティングがあり得る受光器対を示す図である。

【図2】従来の量子暗号である4偏光状態暗号を説明するための図である。

【図3】図2に示す4偏光状態暗号におけるコーディング法およびビット値との対応する偏光状態を示す図である。

【図4】従来の量子暗号である2コヒーレント状態暗号を説明するための図である。

【図5】従来の量子暗号である2コヒーレント状態暗号を説明するための図である。

【図6】従来の量子暗号である時間差干渉暗号を説明するための図である。

【図7】従来の量子暗号である二光子干渉暗号を説明するための図である。

【符号の説明】

1 送信者

2 受信者

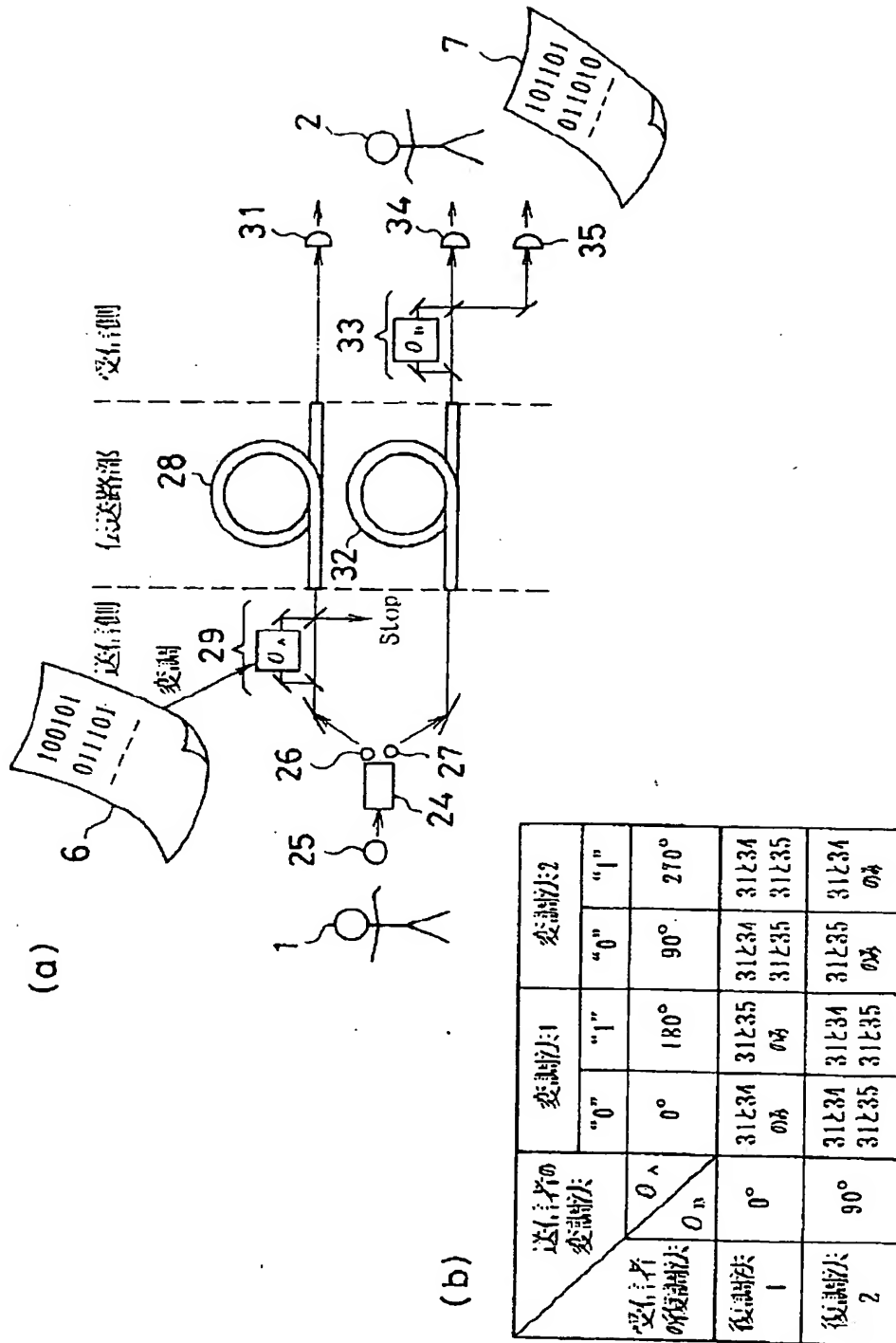
25 ポンプ光子

28, 32 光ファイバ

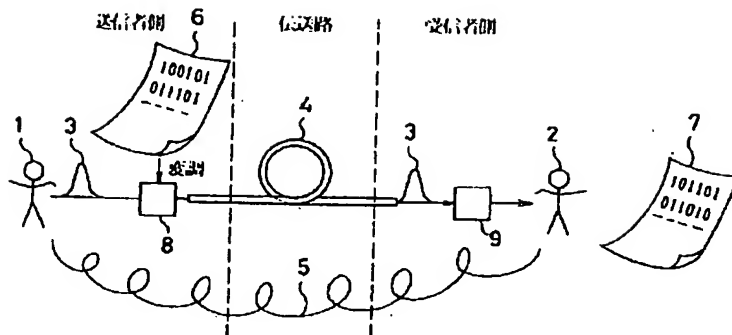
29, 33 マッハツェンダー型遅延

31, 34, 35 受光器

【図1】



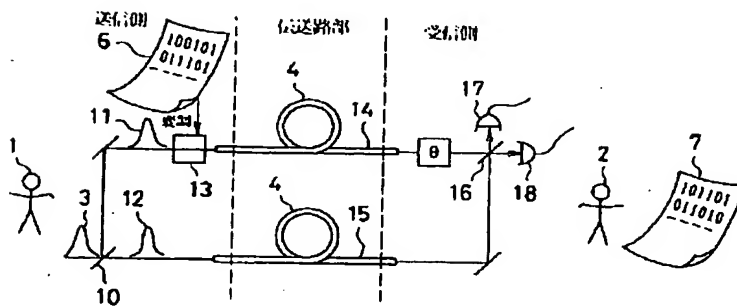
【図 2】



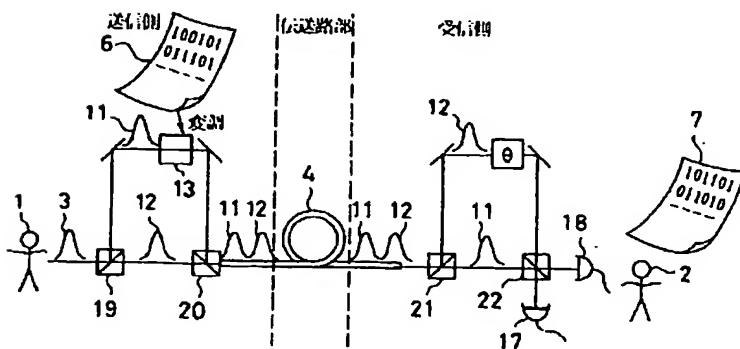
【図 3】

	ビット "0"	ビット "1"
直線偏光 コーディング	↔	↑
P偏光 コーディング	○	○

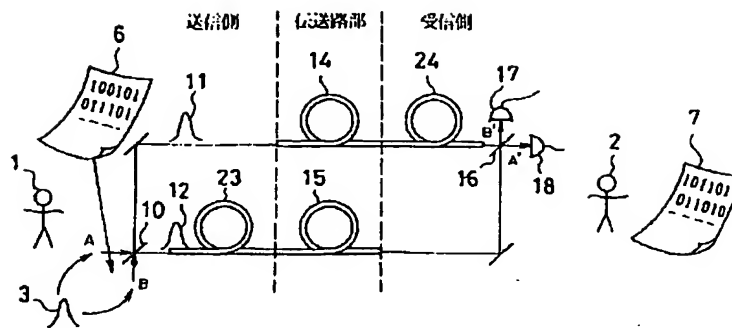
【図 4】



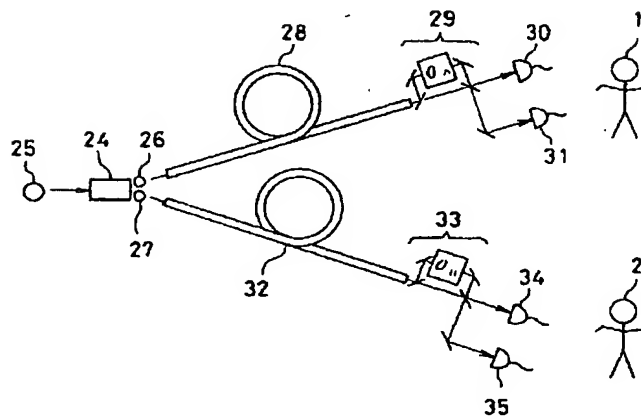
【図 5】



【図 6】



【図 7】



フロントページの続き

(51)Int.Cl.⁶

H 0 4 L 9/08
9/38

識別記号

庁内整理番号

F I

H 0 4 L 9/00

技術表示箇所

6 0 1 C
6 9 1